## POINT XIII

## DEFENDANT REQUEST THAT THE SURREPTITIOUS RECORDING OF HIS CONVERSATION WITH ALLEGED CO-DEFENDANTS IN THE RENTED MINIVAN VIOLATED THE FOURTH AND FIFTH AMENDMENTS OF THE CONSTITUTION

Whether the recording constitutes an unreasonable search in violation of the Fourth Amendment Defendant states that his Fourth Amendment rights to be free from unreasonable search were violated when agents surreptitiously recorded his conversation in a minivan rented by Defendant Mr. Gatson. Defendant contends that the Fourth Amendment and Title III of the Omnibus Crime Control and Safe Streets Act of 1968 "**Title( III"), 18 U.S.C. § 2511**, forbid the recording of his conversation without a warrant or their consent.

The Fourth Amendment provides: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause[.]" **U.S. Const. amend. IV**. A search within the meaning of the Fourth Amendment occurs only when "a reasonable expectation of privacy" exists, and a defendant who objects to a search bears the burden of demonstrating that a reasonable expectation of privacy was violated by the search. **See United States v. French, 291 F.3d 945, 951 (7th Cir.2002); United States v. Ruth, 65 F.3d 599, 604 (7th Cir.1995).**

It is well-established that electronic surveillance can constitute a search for the purposes of the Fourth Amendment. **See Katz v. United States, 389 U.S. 347, 353 (1967).** Title III, the federal wiretap law, limits the government's ability to eavesdrop on communications a person expected to keep private without a wiretap warrant. **Matter of John Doe Trader No. One, 894 F.2d 240, 242 (7th Cir.1990).** The legislative history of Title III indicates that the "expectation of privacy" it protects is "intended to parallel the 'reasonable expectation of privacy' test created by the Supreme Court in **Katz v. United States."** Id.

In Justice Harlan's oft-quoted concurrence, he stated that "there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the

expectation be one that society is prepared to recognize as 'reasonable.' " **Katz, 389 U.S. at 361 (Harlan, J., concurring).**

The first prong of the **Katz** standard is whether the individual who claims his Fourth Amendment rights have been violated has demonstrated an actual subjective expectation of privacy. "In determining whether a defendant held a subjective expectation of privacy, this Court should look at the defendant's efforts to conceal and keep private that which was the subject of the search." **United States v. Villegas, 495 F.3d 761, 767 (7th Cir.2007); see also United States v. Yang, 478 F.3d 832, 835 (7th Cir.2007)**

The second prong of the **Katz** test concerns whether Defendants' subjective expectation of privacy was objectively reasonable. A finding that an expectation of privacy is reasonable "recognizes the everyday expectations of privacy that we all share." **Minnesota v. Olson, 495 U.S. 91, 98 (1990).** The "inquiry into whether a defendant's expectation of privacy was reasonable is necessarily fact dependent, and 'whether a legitimate expectation of privacy exists in a particular place or thing' must be determined on a case-by-case basis." **Villegas, 495 F.3d at 767 (quoting United States v. Waller, 426 F.3d 838, 844 (6th Cir.2005)) (citing United States v. Smith, 978 F.2d 171, 180 (5th Cir.1992))**.

Defendant states that it "is not dispositive that the conversation took place in a rented vehicle" because the Fourth Amendment protects people, not places. "Determining whether an expectation of privacy is 'legitimate' or 'reasonable' necessarily entails a balancing of interests." Id. The Government has failed to explain in its Affidavit what interests justified an intrusion into Defendants' expectation of privacy within the rented van. The more intrusive the search is, the "more insistent" courts should be that a warrant be obtained. **United States v. Torres, 751 F.2d 875, 882 (7th Cir.1984)**. It is "unarguable" that surreptitious video and audio surveillance is "exceedingly intrusive."

Considering the circumstances, the Defendants' "expectations of freedom from intrusion" into his conversation were unreasonable. **See Katz, 389 U.S. at 361 (Harlan, J., concurring).** The officers infringed on Defendants' reasonable expectation of privacy by using hidden recording devices

without obtaining a warrant with probable cause and thus violated Defendants' basic Fourth Amendment rights. Defendant contends that he had a reasonable expectation of privacy in his conversation in the rented minivan, and thus the recording of his conversation should be **SUPPRESSED.**

**POINT XIIII**

**THE BERGEN COUNTY PROSECUTOR'S OFFICE GIVES NO SPECIFIC EXPLANATION IN ANY OF THE CSLI APPLICATION FOR WHY 120 DAYS OF CSLI IS SOUGHT**

The wiretap Applications in this matter are part of an investigation into Burglaries that occurred on specific days; there are no allegations in the wiretap Applications that these crimes is connected to any other crimes.The Bergen County Prosecutor's office never state in the wiretap Affidavit how the target phone numbers were aquired; or how the target phones suspected to be owned by the Defendant or co-conspirators. The Bergen County Prosecutor's Office wiretap applications also has failed to inform this Court through it's affidavits when, where or how was this information relayed to them that the Defendant and Co-Conspirators were allegedly using there cell phones to commit these alleged Burglaries.

The Bergen County Prosecutor's office has not shown in there Affidavits why CSLI for such a broad timespan is either relevant or material, let alone both, to the investigation. The underlying investigation is focused on a series of Burglaries that, according to the "specific and articulable facts" in the Applications, occurred over the course of slightly under a year. No explanation was given why the Bergen County Prosecutor's Office received additional months of CSLI. If the Bergen County Prosecutor's Office is simply trying to tie the suspects to the scenes of the Burglaries, all that must be done is to ask for CSLI that is contemporaneous to the Burglary dates. The Bergen County prosecutor's Office failed to give a good reasons to seek the CSLI for a larger timeframe-- and the Court cannot simply infer what the purpose may be. The Bergen County Prosecutors Office has failed to show that the CSLI is "relevant and material" to the investigation.

A second and independent reason that these Applications are overbroad is that they received CSLI 24/7 for all 120 days. Even assuming that the Bergen County Prosecutor's Office representations

about the limited scope of the CSLI are accurate and that the CSLI really would be limited to incoming or outgoing phone calls. It is too much for the Court to infer that, for example, CSLI after midnight is "relevant and material" to the investigation. To the extent that it is possible for the government to show that CSLI at all times of the day is relevant and material, here the government has failed to provide the necessary factual justification. The targets of these Burglaries only operate at set times of day, and the Bergen County Prosecutor's Office was aware of what time of day these crimes occurred. Even if CSLI outside of these specific timeframes would help provide a necessary context for the Bergen County Prosecutor's Office to better understand the suspects' movements in relation to these crimes, the Bergen County Prosecutor's Office failed to make it's case and provide "specific and articulable facts" supporting such broad CSLI collection. A request for CSLI largely untethered from the temporal aspects of the crime that is being investigated cannot be sufficiently "relevant and material" to warrant disclosure under **§ 2703(d)** unless some explanation is provided for the demand for so much apparently irrelevant CSLI.

The Bergen County Prosecutor's Office is allegedly investigating specific Burglaries that targeted homes; if the purpose of obtaining the CSLI is to determine, for example, whether the suspect carried out surveillance prior to the crime, there should be a specific timeframe for which the government is seeking its information-one that has some temporal connection to the crime. As with the other Applications, it is too much for the Court to infer from these wiretap applications that all CSLI for every minute of the 7 days 24/hrs a day is "relevant and material" to the investigation.

Allegations that an individual may have been involved in a specific crime on a specific date and at a specific time are insufficient to allow the 30 days, 60 days, 90 days or even 120 days--of CSLI sought in these wiretap Applications. Instead, there must be "specific and articulable facts" to demonstrate why all of the CSLI the Begren County Prosecutor's Office received was "relevant and material" to the investigation. The burden is on the government to justify the **§ 2703(d)** requests, and it has failed to adequately do so here.

## POINT XV
## THE BERGEN COUNTY PROSECUTOR'S OFFICE WAS ILLEGALLY TRACKING THE DEFENDANT

Continuous and Contemporaneous monitoring of cell site location data is tantamount to tracking, a form of surveillance Congress separately treated in **ECPA**. As originally drafted, the law expressly paired tracking devices and pen registers in the same title, setting forth procedures for the issuance of court orders allowing their installation and use. In its final form, only two provisions dealing with tracking devices were retained: Section **3117(a),** which permitted the installation of tracking devices which may move from district to district; and Section **3117(b),** which broadly defined tracking device to mean "an electronic or mechanical device which permits the tracking of the movement of a person or object." Subsequently, Congress approved amendments to **Rule 41** specifying the procedural requirements for a tracking device warrant. Among those requirements are probable cause, a 45-day duration period, return to the designated magistrate judge, and notice to the targeted person. **Rule 41(a)(2)(E)** expressly incorporates the definition of tracking device from the Tracking Device Statute. Given this detailed regime for location tracking, there is no reason to suspect that Congress ever intended the SCA to open a back door for law enforcement to employ the same surveillance technique under different (and less rigorous) standards.

The cell-site-location records at issue here currently enable the tracking of the vast majority of Americans. Thus, the collection of cell-site-location records effectively enables "mass" or "wholesale" electronic surveillance, and raises greater Fourth Amendment concerns than a single electronically surveilled car trip. This further supports the Defendant's argument that cell-phone users maintain a reasonable expectation of privacy in long-term cell-site-location records and that the Government's obtaining these records constitutes a Fourth Amendment search. As the Supreme Court recently observed in its landmark cell phone search case:

**The term "cell phone" is itself misleading shorthand: many of these devices are in fact**

**minicomputers that also have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers. Or, just as easily, "the world's most effective tracking devices."**

The SCA is not an appropriate vehicle for continuous monitoring of prospective cell phone location data. The same holds true for recent decisions in other districts, like **Smartphone**. Whether or not cell site data is ultimately held worthy of Fourth Amendment protection, the Tracking Device Statute and **Rule 41** of the Federal Rules of Criminal Procedure have already struck a fair balance between law enforcement and privacy concerns, and that balance is entitled to respect as the considered judgment of Congress. Because the government's argument seeks to bypass the only legitimate route Congress has mapped out for location tracking surveillance.

## POINT XVI
## THE GOVERNMENT'S APPLICATION OF § 2703(d), IS MISPLACED

The cell-site-location records at issue here currently enable the tracking of the vast majority of Americans. Thus, the collection of cell-site-location records effectively enables "mass" or "wholesale" electronic surveillance, and raises greater Fourth Amendment concerns than a single electronically surveilled car trip. This further supports the court's conclusion that cell-phone users maintain a reasonable expectation of privacy in long-term cell-site-location records and that the Government's obtaining these records constitutes a Fourth Amendment search.

In the pending Affidavit, the Bergen County Prosecutor's Office requested essentially a court subpeona in support of a very broad and invasive search affecting likely at least hundreds of individuals in violation of the Fourth Amendment. The Constitution mandates that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." **U.S. Const. amend. IV**. It further provides that "no Warrants shall issue, but upon probable cause." **Id.; see also Fed.R.Crim.P. 41**. There is nothing from the Government in its argument nor in the Bergen County Prosecutor's Office wiretap affidavits to support the position that the "specific and articulable facts" standard and **§ 2703(d)** apply to cell tower dumps.

In matters regarding electronic surveillance, the United States Attorney often relies on a governmental publication for guidance. See **United States Department of Justice, Electronic Surveillance Manual (rev. 2005), available at www.7/8justice.7/8gov/7/8criminal/7/8foia/7/8 docs/7/8elec-7/8sur-7/8manual.7/8pdf.** Regarding applications pursuant to **§ 2703(d),** it directs federal prosecutors to make such applications:

> **appl[y] to the court for an order, pursuant to § 2703(d), directing (provider of electronic communication service ...) to disclose the (choose as appropriate: name, address, local and long distance telephone connection records, or records of session times and durations; length of service [including start date] and type of service utilized; telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; [and] means and source of payment for such service.**

The applicant then is to certify "that it is believed that the subjects of the investigation are using the (choose as appropriate: telephone or instrument number; other subscriber number or identity ...) in furtherance of the subject offenses; and that the information sought is relevant and material to an ongoing investigation." Id. According to the Department of Justice's own guidance, its attorneys must know the telephone number or other similar identifier such as an ESN, MEIN, MIN, SIM, MSISDN, IMSI, or IMEI to obtain a court order pursuant to **§ 2703(d).**

Even if the Government tries to use **§ 2703(d),** to try and fill the holes in the Bergen County Prosecutor's Office wiretap Affidavit, The only problem is both the Government and the Bergen County Prosecutor's Office failed to submit an application pursuant to **§ 2703(d)** to a Federal Magistrate or State Judge with all of these ESN, MEIN, MIN, SIM, MSISDN, IMSI, or IMEI identifiers.

The Government and Bergen County Prosecutor's Office both have failed to submit an application pursuant to **§ 2703(d),** or even a affidavit pursuant to Rule 41 of the Federal Rules of Criminal Procedure demonstrating probable cause supporting the request for the records. Courts have concluded that such requests must be made based on the probable cause standard. **See In the Matter of the Application of the United States for an Order Pursuant to 18 U.S.C. § 2703(d), 930 F.Supp.2d at 701-02, 2012 WL 4717778.**

Although the use of a court-sanctioned cell tower dump invariably leads to such information being provided to the Bergen County Prosecutor's Office and Government, in order to receive such data, the Bergen County Prosecutor's office and Government at a minimum should have presented a protocol to address how to handle this sensitive private information. This failure to address the privacy rights for the Fourth Amendment concerns of these innocent subscribers whose information will be compromised as a request of the cell tower dump is another factor warranting a **Suppression**.

## POINT XVII
## AGENTS ILLEGALLY SEARCHED AND SEIZED DEFENDANT'S CELL PHONE

The issue presented in this motion is whether the search of Defendant's cell phone without a warrant was authorized under the Fourth Amendment based upon the "search incident to arrest" exception to the warrant requirement. In the face of this authority, Defendant points to **Arizona v. Gant, 556 U.S. 332, 129 S.Ct. 1710, 173 L.Ed.2d 485 (2009),** as having changed the calculus used to determine the applicability of this exception to seizure of cell phones. Defendant also highlights recent authority in the wake of **Gant** that limits the warrantless search of cell phone data seized incident to arrest. **See United States v. Wurie, No. 11-1792, 728 F.3d 1, 13 (1st Cir.2013)** (holding "that the search-incident-to-arrest exception does not authorize the warrantless search of data on a cell phone seized from an arrestee's person, because the government has not convinced us that such a search is ever necessary to protect arresting officers or preserve destructible evidence."); **Smallwood v. State, 113 So.3d 724, 740 (Fla.2013)** (holding "that, while law enforcement officers properly separated and assumed possession of a cell phone from Smallwood's person during the search incident to arrest, a warrant was required before the information, data, and content of the cell phone could be accessed and searched by law enforcement.").

Several factors, however, make this case more difficult. For **one** thing, this case involves the extraction and seizure of data and private information from a cell phone. A **second** factor is that the search of the cell phone, while roughly contemporaneous with Defendant's arrest, booking, and interview,

was conducted at the agents' offices, outside of Defendant's presence, after Defendant had been taken into custody and removed to another location for booking and interview, and involved much more than just a limited search for the phone's log history or recent calls.

Defendant's cell phone was seized from his hotel room incident to his arrest under a arrest warrant. Defendant does not attack the seizure of the phone; instead, he challenges the search of the phone that was conducted after the arrest, away from the scene of the arrest, outside of Defendant's presence at the agent's office, where the agent plugged a device into the phone and extracted the data from the phone itself and from its "SD card."

Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse. Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person. The term "cell phone" is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.

One of the most notable distinguishing features of modern cell phones is their immense storage capacity. Before cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy. **See Kerr, Foreword: Accounting for Technological Change, 36 Harv. J.L. & Pub. Pol'y 403, 404-405 (2013).** Most people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read--nor would they have any reason to attempt to do so. And if they did, they would have to drag behind them a trunk of the sort held to require a search warrant in **Chadwick, supra,** rather than a container the size of the cigarette package in **Robinson**.

The current top-selling smart phone has a standard capacity of 16 gigabytes (and is available with up to 64 gigabytes).

Sixteen gigabytes translates to millions of pages of text, thousands of pictures, or hundreds of videos. **See Kerr, supra, at 404; Brief for Center for Democracy & Technology et al. as Amici Curiae 7-8.** Cell phones couple that capacity with the ability to store many different types of information: Even the most basic phones that sell for less than $20 might hold photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on. **See id., at 30; United States v. Flores-Lopez, 670 F.3d 803, 806 (C.A.7 2012).**

The storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information--an address, a note, a prescription, a bank statement, a video--that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.

Finally, there is an element of pervasiveness that characterizes cell phones but not physical records. Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day. Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception. According to one poll, nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower. **See Harris Interactive, 2013 Mobile Consumer Habits Study (June 2013).** A decade ago police officers searching an arrestee might have occasionally stumbled across a highly personal item such as a diary. **See,e.g., United States v. Frankenberry, 387 F.2d 337 (C.A.2 1967)** (per curiam ). But those discoveries were likely to be few and far between.

Today, by contrast, it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives--from the mundane to the intimate. **See Ontario v. Quon, 560 U.S. 746, 760, 130 S.Ct. 2619, 177 L.Ed.2d 216 (2010).** Allowing the police to scrutinize such records on a routine basis is quite different from allowing them to search a personal item or two in the occasional case.

Although the data stored on a cell phone is distinguished from physical records by quantity alone, certain types of data are also qualitatively different. An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns--perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD. Data on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building. **See United States v. Jones, 565 U.S. ----, ----, 132 S.Ct. 945, 955, 181 L.Ed.2d 911 (2012)** (SOTOMAYOR, J., concurring) ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.").

Mobile application software on a cell phone, or "apps," offer a range of tools for managing detailed information about all aspects of a person's life. There are apps for Democratic Party news and Republican Party news; apps for alcohol, drug, and gambling addictions; apps for sharing prayer requests; apps for tracking pregnancy symptoms; apps for planning your budget; apps for every conceivable hobby or pastime; apps for improving your romantic life. There are popular apps for buying or selling just about anything, and the records of such transactions may be accessible on the phone indefinitely. There are over a million apps available in each of the two major app stores; the phrase "there's an app for that" is now part of the popular lexicon. The average smart phone user has installed 33 apps, which together can form a revealing montage of the user's life. **See Brief for Electronic Privacy Information Center as Amicus Curiae in No. 13-132, p. 9.**

In 1926, Learned Hand observed (in an opinion later quoted in **Chimel** ) that it is "a totally different thing to search a man's pockets and use against him what they contain, from ransacking his house for everything which may incriminate him." **United States v. Kirschenblatt, 16 F.2d 202, 203 (C.A.2).** If his pockets contain a cell phone, however, that is no longer true. Indeed, a cell phone search would typically expose to the government farmore than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form--unless the phone is.

The Agents clearly went beyond merely seizing the phone, examining it to ascertain that it was not a weapon, and preserving it. The Agents took it back to his office and extracted all the data he could extract using a data extraction device. This intrusion was more than minimal.

This is not a case where there was any threat that the arrestee might use the cell phone as a weapon, in view of the fact that the phone had been immediately seized from him, and, secondly, because it was immediately ascertained that it was not a weapon. Nor is this a case where there was any viable threat that the phone data could be remotely wiped or destroyed. Once the officer had possession of the phone it could be immediately shut off or put in "airplane mode" and/or its battery removed, effectively eliminating any possibility of such a remote intrusion pending examination of the phone in a controlled environment. There would have been ample time, in other words, for the agents to obtain a warrant, properly limited in scope, assuming the officers had probable cause to justify the search.

Furthermore, the privacy interests that an individual has in his or her cell phone, given the nature of such phones today, distinguishes it from an individual's wallet, for example, which may be examined immediately upon arrest in order to confirm identity, among other things, or a briefcase, which may contain a weapon, or other dangerous instrumentality, or destructible evidence. Modern cell phones, like Defendant's Cell phone, are in effect mini-computers, and contain contacts, text messages, photographs, calendars, notes and memos, instant messages, voice memos, and e-mail messages--a wealth of private information held within a small digital "container," as it were, but a different kind of container from a crumpled cigarette package or even a footlocker.

As opposed to a foot locker, or a cigarette pack, which are capable of holding other objects, a cell phone is an integrated digital device that holds only data and digitally stored information.

Requiring a warrant in these circumstances before such a search may be conducted does not impair the legitimate interests of the government in ensuring the safety of the arresting officers and the preservation of any evidence. These interests were fully protected in this case by immediately taking the phone from the Defendant's hands incident to his arrest and securing it. At the same time, by requiring a warrant in this situation for the search of the phone, the legitimate privacy interests of the arrestee can be protected, while still permitting the phone to be immediately seized and preserved pending further action.

**CONCLUSION**

Since the time of its framing, "the central concern underlying the Fourth Amendment" has been ensuring that law enforcement officials do not have "unbridled discretion to rummage at will among a person's private effects." **Gant, 556 U.S. at 345, 129 S.Ct. 1710; see also Chimel, 395 U.S. at 767-68, 89 S.Ct. 2034**. Today, many Americans store their most personal "papers" and "effects," **U.S. Const. amend. IV**, in electronic format on a cell phone, carried on the person. Allowing the police to search that data without a warrant any time they conduct a lawful arrest would, in our view, create "a serious and recurring threat to the privacy of countless individuals." **Gant, 556 U.S. at 345, 129 S.Ct. 1710; cf. United States v. Jones, --- U.S. ----, 132 S.Ct. 945, 950, 181 L.Ed.2d 911 (2012)** ("At bottom, we must 'assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.' " **(quoting Kyllo v. United States, 533 U.S. 27, 34, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001)))**.

Thus, the motion to **SUPPRESS** should be **GRANTED**.

**POINT XVIII**

**THE GOVERNMENT FAILED TO PROVIDE A SEARCH PROTOCOL TO ADDRESS THE PARTICULARITY OF THE PLACE TO BE SEARCHED**

**In re Search of Black iPhone** and **In re Search of Odys Loox**, two opinions issued where the Court admonished the government to explain how it intends "to search for each thing it intends to seize

[and] how it will deal with the issue of intermingled documents." **In re Search of Black iPhone, 2014 WL 1045812**. The Government failed to satisfy the particularity requirement of what will be searched and failed to fully explain to the Court how much data for which it does not have probable cause will likely be seized.

The concerns raised by the Defendant, which are repeated in **In re Search of Odys Loox**, are based on the probable cause and particularity requirements of the Fourth Amendment. The Fourth Amendment provides:

**The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.**

**U.S. Const. amend. IV**. Items, such as data, can only be seized if there is probable cause to support their seizure. **See Coolidge v. N.H., 403 U.S. 443, 467, 91 S.Ct. 2022, 29 L.Ed.2d 564 (1971).** With respect to the particularity requirement, the Supreme Court has recognized that it "ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." **Maryland v. Garrison, 480 U.S. 79, 84, 107 S.Ct. 1013, 94 L.Ed.2d 72 (1987).** As a result, "the scope of a lawful search is 'defined by the object of the search and the places in which there is probable cause to believe that it may be found. Just as probable cause to believe that a stolen lawnmower may be found in a garage will not support a warrant to search an upstairs bedroom, probable cause to believe that undocumented aliens are being transported in a van will not justify a warrantless search of a suitcase.' " **Id. at 84-85, 107 S.Ct. 1013 (citing United States v. Ross, 456 U.S. 798, 824, 102 S.Ct. 2157, 72 L.Ed.2d 572 (1982)).** The Government's Application violated both of these provisions.

The Defendant's argument is about the overseizure of data for which there was no probable cause. The Government application fails to indicate how they plan to take and sift through massive amounts of data for which it had **NO** probable cause to seize in the first place. **See In re Search Black iPhone, 2014 WL 1045812**.

The Government also failed to provide an intended search protocol so that the Magistrate could better understand the scope of the warrant it was asked to issue. Whether the target devices would be imaged in full, for how long those images will be kept, and what will happen to data that is seized but is ultimately determined not to be within the scope of the warrant--or, more precisely, these things can only be addressed by a search protocol; after all, the imaging actually occurs as part of the search process.

The government failed to address this same issue in **In re Search of Odys Loox,** There the Government indicated that it would "image these devices and store them until the target/ defendant's appeals and habeas proceedings are concluded." **2014 WL 1063996**. The government was therefore admitting that, even though it had probable cause for only some of the data on the devices, it intended to keep all of the data for an indefinite period of time. That would constitute an unconstitutional seizure, which this Court should not permit. **See United States v. Tamura, 694 F.2d 591, 595 (9th Cir.1982)** ("However, the wholesale seizure for later detailed examination of records not described in a warrant is significantly more intrusive, and has been characterized as 'the kind of investigatory dragnet that the Fourth amendment was designed to prevent.' ") (**citing United States v. Abrams, 615 F.2d 541, 543 (1st Cir.1980)**).

This is important because, if the device will be imaged, then there will be a complete copy of all its data--including the data for which there is no probable cause to seize--that must be accounted for and which ultimately must be purged of data outside the scope of the warrant. The government should have addressed this issue in there application and made clear that the non-relevant data will be deleted from any system images. **See United States v. Hill, 459 F.3d 966, 976-77 (9th Cir.2006)** (holding overbroad a warrant authorizing the "blanket seizure" of computer storage media without sufficiently explaining the process--in that case removing all storage media offsite--to the issuing magistrate).

In a broad manner, describing the Phone and its specific IMEI number certainly describes the "place to be searched" in a particular manner. But an electronic search is not that simple. The Defendant's phone has either 16 GB or 32 GB of flash memory, which could allow storage of up to around two million text documents.

I would think the Government has access to computers that can perform some sort of scans to assist and determine whether it is evidence described by the warrant.

A sufficient search protocol, i.e. an explanation of the scientific methodology which the government failed to use to separate what is permitted to be seized from what is not, will explain to the Court how the government will decide where it is going to search--and it is thus squarely aimed at satisfying the particularity requirement of the Fourth Amendment.

The Defendant is not requiring a search protocol so that it may specify how the warrant is to be executed. Instead, the protocol will explain to the Court how the government intends to determine where it will search (which "parts"--or blocks--of the Phone's NAND flash drive) and how those decisions with respect to how the search will be conducted will help limit the possibility that locations containing data outside the scope of the warrant will be searched (which is the intermingled documents problem,) **see In re Search Black iPhone, 2014 WL 1045812**.

One other point worth noting, In the physical world, a search of an entire file cabinet or building for a particular document is constitutionally permissible only because there is no way to know with any certainty ahead of time how the search location can be narrowed so that only the specific folder containing the document will be searched. **See United States v. Burgess, 576 F.3d 1078, 1094 (10th Cir.2009)** ("One would not ordinarily expect a warrant to search filing cabinets for evidence of drug activity to prospectively restrict the search to 'file cabinets in the basement' or to file folders labeled 'Meth Lab' or 'Customers.' ").

In such instances, the textual admonitions of the Fourth Amendment must give way to the practical reality of how the search must be conducted. **Tamura, 694 F.2d at 595** ("It is true that all items in a set of files may be inspected during a search, provided that sufficiently specific guidelines for identifying the documents sought are provided in the search warrant and are followed by the officers conducting the search.").

The digital world however, is entirely different. For example, sophisticated search tools exist, and

those search tools allow the government to find specific data without having to examine every file on a hard drive or flash drive.

When searching electronic devices to seize the data, the potential for abuse has never been greater: it is easy to copy them and store thousands or millions of documents with relative ease. But, by using search tools, there is also the potential for narrowing searches so that they are more likely to find only the material within the scope of the warrant. It is, of course, also in the government's best interest to do so, as it would be a waste of resources to, for example, search file by file looking for data in the scope of the warrant--assuming that, on a 16 or 32 GB flash drive.

The government failed to explain how it is going to conduct this search to minimize the risk that files outside the scope of the warrant will be discovered. As the Ninth Circuit has made clear, "the reality that over-seizing is an inherent part of the electronic search process" requires this Court to "exercise 'greater vigilance' in protecting against the danger that the process of identifying seizable electronic evidence could become a vehicle for the government to gain access to a larger pool of data that it has no probable cause to collect." **United States v. Schesso, 730 F.3d 1040, 1042 (9th Cir.2013) (citing United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1177 (9th Cir.2010)**. An appropriate search protocol is the answer to protecting against the government searching data on an electronic device when it has no right to search that data.

**CONCLUSION**

By the government failing to explain how the search was conducted, or how the government intended to limit its search of data outside the scope of the warrant, this warrant should be **SUPPRESSED.**

**POINT XVIIII**
**THE GOVERNMENT FAILED TO PROVIDE A SUFFICIENT SEARCH PROTOCOL**

The present matter is a direct sequel to the opinion in **In re Search of Black iPhone**. The Government seized Defendant's laptop and tablet, But failed to "explain to the Court what the basis for

probable cause was to search for each thing it seized [and] how it will deal with the issue of intermingled documents." **In re Search of Black iPhone, --- F.Supp.2d at ----, 2014 WL 1045812**. The Defendant states that this was a complete lapse of failure on the Government's part for failing to give some indication of how the search will proceed.

The Governments application is void when it comes to answering questions like: Will all of these devices be imaged? For how long will these images be stored? Will a dedicated computer forensics team perform the search based on specific criteria from the investigating officers of what they are looking for, or will the investigating officers be directly involved? What procedures will be used to avoid viewing material that is not within the scope of the warrant?

The government has not, addressed any of these concerns nor explained how the search will occur and how the government will avoid overseizure by avoiding keeping documents and other information outside the scope of **18 U.S.C. 2314**. There also is no indication in the Governments application, how, that the original files will be returned.

The Government's application gives you the impression that a computer forensic specialist will image and search the drives, but there is no explanation of what that person's relationship is with the team investigating the underlying crime and whether the investigating officers will be directly involved in the search. Second, the government fails to inform the Magistrate ifonly copies of the data will be returned and thus the Government keeps the originals (unless the entire device contains no such relevant data). Third, will the government be "print[ing]" materials for evidence purposes or make electronic copies of documents. Even if non-relevant documents "will not be shown to anyone else or printed for any purpose," the real question is what will happen with electronic copies--which it seems the government will retain indefinitely.

Although the above paragraphs raises issues that need clarification, there are two larger systemic problems. First, the government intends to wholly image these devices and store them "until the target/ defendant's appeals and habeas proceedings are concluded." This is unacceptable.

The government cannot keep data that is outside the scope of the warrant. Accordingly, that data must be either returned or destroyed, and it certainly cannot be kept indefinitely pending appeal. **See In re Search of Black iPhone, --- F.Supp.2d at ----, 2014 WL 1045812** ("Will such information be returned, destroyed, or kept indefinitely? The government must specify what will occur--although it is admonished that any response other than 'the information will be returned or, if copies, destroyed' within a prompt period of time will likely find any revised application denied.").

Another major issue the government failed to provide an actual search protocol. The government failed to instruct the Court how it intended to conduct the search. **See In re Search of Black iPhone, --- F.Supp.2d at ----, 2014 WL 1045812** ("But the Court will require the government to give some indication of how the search will proceed ... What procedures will be used to avoid viewing material that is not within the scope of the warrant?").

By the government not providing a search protocol which would have informed the Magistrate of technical overview of how they planned or conducted the search, this search was in essence a "general, exploratory rummaging in a person's belongings" that the Fourth Amendment prohibits. **See Coolidge v. N.H., 403 U.S. 443, 467, 91 S.Ct. 2022, 29 L.Ed.2d 564 (1971).**

**CONCLUSION**

By the government failing to explain how the search was conducted, or how the government intended to limit its search of data outside the scope of the warrant, this warrant should be **SUPPRESSED.**

**POINT XX**
**The Government Lacked Probable Cause for Information Relating to Third Parties**

The Supreme Court has recognized two constitutional protections served by the warrant requirement of the Fourth Amendment. "First, the magistrate's scrutiny is intended to eliminate altogether searches not based on probable cause.

The premise here is that any intrusion in the way of search or seizure is an evil, so that no intrusion

at all is justified without a careful prior determination of necessity." **Coolidge v. New Hampshire, 403 U.S. 443, 467, 91 S.Ct. 2022, 29 L.Ed.2d 564 (1971**). Thus, it is this Court's duty to reject any applications for search warrants where the strict standard of probable cause has not been met. Second, "those searches deemed necessary should be as limited as possible. Here, the specific evil is the 'general warrant' abhorred by the colonists, and the problem is not that of intrusion per se, but of a general, exploratory rummaging in a person's belongings." Id. These twin inquiries are inseparably intertwined by the text of the Fourth Amendment: **"no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV**. To follow the dictates of the Fourth Amendment and avoid issuing a general warrant, a court must be careful to ensure that probable cause exists to seize each item specified in the warrant.

Here, there was certainly **NO** probable cause to search and seize items in Mr. Gatson's Instagram account because there was **NO** probable cause to believe that it contained evidence indicating his alleged motive in committing **18 U.S.C. 2314** and whether he conspired with anyone.

The government's application, however, wholly failed to provide any explanation whatsoever for why there was probable cause to search and seize information about third parties. Without probable cause to seize this material, this Court cannot allow a warrant authorizing its seizure.

In addition to the lack of probable cause, a separate constitutional concern arises from the government's apparent attempt to obtain information about any of Mr. Gatson's instagram groups, or friends that may have joined. The plain language of this request would require Instagram to turn over membership lists, which implicates the right to free association found in the First Amendment. **See NAACP v. Alabama, 357 U.S. 449, 462, 78 S.Ct. 1163, 2 L.Ed.2d 1488 (1958)** ("This Court has recognized the vital relationship between freedom to associate and privacy in one's associations.").

Whether these groups were potentially political advocacy groups is immaterial, as this Constitutional protection "pertain[s] to political, economic, religious or cultural matters, and state

action which may have the effect of curtailing the freedom to associate is subject to the closest scrutiny." **Id. at 460-61, 78 S.Ct. 1163**.

Depending on what the government found after a search of Mr. Gatson's Instagram account, probable cause could exist to learn more information about another individual or a group. But no such probable cause existed for the initial foray into Mr. Gatson's Instagram profile, and it was therefore premature for the government to seek so much information about third parties.

The government's application "casts a remarkable dragnet over communications that surely have nothing to do with this case, including those to and from third parties, who will never know of the government's seeing their communications with Mr. Gatson about unrelated matters." **See In the Matter of the Search of Information associated with Facebook Account: http://facebook.com/[John.Doe] that is stored at premises controlled by Facebook, Inc., 13-MJ-485, slip op. at 2 (D.D.C. June 14, 2013) (Facciola, M.J.) (sealed).** Individuals may voluntarily share their information with Instagram, but the government, by seeking a search warrant, justly reasons that probable cause for searching within a Instagram account is still a constitutional necessity, particularly when it will have to see third party communications that are innocuous and irrelevant and sent by persons who could not possibly have anticipated that the government would see what they have posted.

It may be strange that a court would even need to raise concerns about what the government might do with information that it collects that falls outside the scope of a search and seizure warrant. After all, such collection would appear to be a per se violation of the Fourth Amendment. Due to the current "reality that over-seizing is an inherent part of the electronic search process" that gives the government "access to a larger pool of data that it has no probable cause to collect," this Court is obliged to create minimization procedures to limit the possibility of abuse by the government. **United States v. Schesso, 730 F.3d 1040, 1042 (9th Cir.2013) (citing United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1177 (9th Cir.2010). See also Comprehensive Drug Testing, 621 F.3d at 1178 (Kozinksi, J. concurring)** (suggesting procedures magistrate judges should follow to prevent "turning all warrants for digital data into general warrants").

Part of the problem here comes from **Rule 41**, which creates a two-step procedure for the search and seizure of electronic information that necessarily allows seizing far more information than a warrant specifies. **See Fed. R. Crim. P. 41(e)(2)(B).** Under that Rule, a warrant "may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or other information consistent with the warrant." Id. According to the 2009 notes from the Advisory Committee, this procedure was codified because "it is often impractical for law enforcement to review all of the [electronic] information during execution of the warrant at the search location .... officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant." **Fed. R. Crim. P. 41**.

It is with the two-step procedure in **Rule 41** in mind that the government has created the fiction that, although a great deal of information will be disclosed to them by Instagram, they will only "seize" that which is specified in the warrant. **See generally In re Applications for Search Warrants for Information Associated with Target Email Accounts/Skype Accounts, Nos. 13-MJ-8163, 13-MJ-8164, 13-MJ-8165, 13-MJ-8166, 13-MJ-8167, 2013 WL 4647554 (D.Kan. Aug. 27, 2013) (" In re App.")** (the government's search warrant applications used the same bifurcated distinction between information disclosed and information "seized").

The current two-step procedure that has been codified in **Rule 41** is born from an attempt to balance the practical needs of the government with the requirements of the Fourth Amendment. Without question, the requirements of the Fourth Amendment are paramount; since the government failed to create a practical way to perform electronic searches and seizures that does not violate the Fourth Amendment, then they are simply not entitled to that information.

The Government failed to provide some safeguards in place to prevent the government from collecting and keeping indefinitely information to which it has no right. The basis in the Fourth Amendment for those orders, and the minimization order here, is that the government had not established probable cause for the entirety of Mr. Gatson's Instagram account, The Government violated the Defendant's

Fourth Amendment rights by for the government to permanently seizing all contents, records, and other data related to the Defendant's account.

Since the 2009 amendment to **Rule 41**, there has been a sea change in the manner in which computers, which now contain enormous amounts of data, are searched with technology assisted review replacing other forms of searching, including the once thought gold standard of file-by-file and document-by-document review. Thus, the premise of the 2009 amendment--that law enforcement had to open every file and folder to search effectively--may simply no longer be true. The defendant finds it hard to believe that a law enforcement agency of remarkable technical ability such as the FBI is opening every file and folder when it seizes a computer that contains a terabyte of data. The Defendant cannot imagine that the F.B.I. has the time or personnel to do it, nor see any reason to do it when there are more efficient means to do what its agents have to do.

**CONCLUSION**

The Supreme Court has recognized two constitutional protections served by the warrant requirement of the Fourth Amendment.

"First, the magistrate's scrutiny is intended to eliminate altogether searches not based on probable cause. The premise here is that any intrusion in the way of search or seizure is an evil, so that no intrusion at all is justified without a careful prior determination of necessity." **Coolidge, 403 U.S. at 467, 91 S.Ct. 2022**. It is this Court's duty to reject any applications for search warrants where the standard of probable cause has not been met. Second, "those searches deemed necessary should be as limited as possible.

Here, the specific evil is the 'general warrant' abhorred by the colonists, and the problem is not that of intrusion per se, but of a general, exploratory rummaging in a person's belongings."Id. To follow the dictates of the Fourth Amendment and to avoid issuing a general warrant, a court must be careful to ensure that probable cause exists to seize each item specified in the warrant application.

**POINT XXI**

**THE GOVERNMENTS APPLICATION TO SEARCH DEFENDANT'S EMAILS WERE UNCONSTITUTIONAL BECAUSE BECUASE THE GOVERNMENT FAILED TO SHOW PROBABLE CAUSE TO SEARCH THE CONTENTS OF ALL EMAILS EVER SENT TO OR FROM THE DEFENDANT'S ACCOUNT**

Any e-mails that are turned over to the government are unquestionably "seized" within the meaning of the Fourth Amendment. **See In re Search of Apple E-mail, 2014 WL 945563, (citing Brower v. Cnty. of Inyo, 489 U.S. 593, 596, 109 S.Ct. 1378, 103 L.Ed.2d 628 (1989)** (noting that a "seizure" occurs when there is "an intentional acquisition of physical control"). Although the Supreme Court has never specifically defined what constitutes a seizure in the electronic world, it has stated that, with regard to physical items, a " 'seizure' of property only occurs when there is some meaningful interference with an individual's possessory interests in that property." **United States v. Jacobsen, 466 U.S. 109, 113, 104 S.Ct. 1652, 80 L.Ed.2d 85 (1984).**

A seizure of property occurs when e-mails are copied and taken by the government without the owner's consent because an individual's "possessory interest [in the e-mails] extends to both the original and any copies made from it." **Orin Kerr, Fourth Amendment Seizures of Computer Data, 119 Yale L.J. 700, 703 (2010).** After all, when a copy is made, "the person loses exclusive rights to the data," id., and it is at that time that the owner's property interest in the e-mail is affected. This reality has been assumed, if not stated outright, in the numerous cases that acknowledge that e-mails turned over to the government by an electronic communications service provider are "seized." **See, e.g., In re Search of Target Email Address, 2012 WL 4383917, United States v. Taylor, 764 F.Supp.2d 230, 237 (D.Me.2011); United States v. Bickle, No. 10-CR-00565, 2011 WL 3798225 (D.Nev. July 21, 2011); United States v. Bowen, 689 F.Supp.2d 675, 684 (S.D.N.Y.2010).**

To conclude otherwise would yield unsatisfactory results. First, if copying were not considered "seizing," that would suggest the irrelevance of the Fourth Amendment to that act:

**If copying data is not a seizure, then copying cannot logically be regarded as a search and it does not violate an expectation of privacy. It is possible to copy files without examining the files. Therefore, if copying is not a seizure, it is outside the scope of the Fourth Amendment's reasonableness requirements and is an activity which can be conducted at will, requiring neither the justification of a warrant nor an exception to the warrant requirement. This is not a satisfactory result. Copying has an effect upon the "ownership" rights of the party whose information is copied.**

**Susan Brenner and Barbara Frederiksen, Computer Searches and Seizures: Some Unresolved Issues, 8 Mich. Telecomm. & Tech. L.Rev. 39, 113 (2002).** The Defendant believes that, if the act of copying e-mail is not a seizure, then the Fourth Amendment is powerless to prevent the wholesale copying of every single e-mail ever sent, a result that no court could ever reasonably embrace. It would also render hollow the Sixth Circuit's holding in **United States v. Warshak, 631 F.3d 266, 285-88 (2010),** that there is a reasonable expectation of privacy with respect to one's e-mails--even though those e-mails were copied by an electronic communications service provider and given to the government. **Id. at 283.**

A seizure could only occur if the actual hard drive that contains the target e-mail account, is physically taken by the government. This ignores the reality that "[h]ardware is increasingly fungible" and that what really matters--and what the owner of the e-mails actually has a possessory interest in--"is the data." **Fourth Amendment Seizures of Computer Data, 119 Yale L.J. at 712.**

A focus on hardware instead of data, in determining when a seizure occurs, would therefore miss the mark and ignore fundamental realities about how computers are actually used. **See In re Southeastern Equipment Co. Search Warrant, 746 F.Supp. 1563, 1576 (S.D.Ga.1990)** ("As the LeClair Court pointed out, it is the information itself, not the paper and ink or tape recorder or other copying utensil, that is actually seized.") **(citing LeClair v. Hart, 800 F.2d 692, 696 n. 5 (7th Cir.1986)).**

Even if the government characterizes the act of copying e-mails as a seizure by noting that it will "seize" some of the copied e-mails after the search is complete. It is, after all, seeking a "search and seizure warrant." **See Fed.R.Crim.P. 41.**

The problem with the government's Application is that it fails to specify with particularity what it intends to seize--therefore the government was allowed to seize large quantities of e-mails for which it has not established probable cause and which are outside the scope of Attachment B.

This Court has an affirmative obligation to "prevent[ ] the seizure of one thing under a warrant describing another." **See Andresen v. Maryland, 427 U.S. 463, 479, 96 S.Ct. 2737, 49 L.Ed.2d 627 (1976) (citing Stanford v. Texas, 379 U.S. 476, 485, 85 S.Ct. 506, 13 L.Ed.2d 431 (1965)).**

Here, the warrant fails to describe certain emails that are to be seized--even more troubling is the government hasn't established probable cause for any of the Defendant's emails. This is unconstitutional because "[t]he government simply has not shown probable cause to search the contents of all emails ever sent to or from the Defendant's account." **See In re Search of Target Email Address, 2012 WL 4383917**. As Judge David J. Waxse wisely analogized, if this were the physical world, it would be akin to "a warrant asking the post office to provide copies of all mail ever sent by or delivered to a certain address so that the government can open and read all the mail to find out whether it constitutes fruits, evidence or instrumentality of a crime. The Fourth Amendment would not allow such a warrant." Id. The Defendant agrees.

The government "abused the two-step procedure under **Rule 41**". The government cannot pretend that the seizure only occurs after it has searched and separated the relevant e-mails from the irrelevant ones.

Unlike a search of a hard drive or cell phone, there is an alternative that, in accordance with the Fourth Amendment, prevents the government from seizing large quantities of data for which it has not established probable cause: Otherwise, if the Court were to Deny the Defendant's request the Government's Application as it is, the government would immediately seize a vast quantity of e-mails to which it is not entitled; in so doing, this Court would in essence be issuing a general warrant.

**CONCLUSION**

The government made no effort to protect the target's Fourth Amendment rights. If the government seizes data it knows is outside the scope of the warrant, it must either destroy the data or return it. It cannot simply keep it. There is no question that the governments Application violates the Fourth Amendment.

## POINT XXII

**Bergen County Judge Honorable Liliana S. DeAvila-Silebi, P.J., Cr. and Bergen County Judge Edward A. Jerejian, J.S.C. granted members of the Bergen County Prosecutor's Office authorization to seize Cell Tower Records and a motor vehicle (Vin#2C4RC1BG3DR74200) and install a tracking device, bugging system should be suppressed because it was outside of there Statutory Jurisdiction**

A search warrant signed by a person who lacks the authority to issue it is void as a matter of law. **United States v. Neerng, 194 F.Supp.2d 620, 627 (E.D.Mich.2002) (citing United States v. Scott, 260 F.3d 512 (6th Cir.2001)).** The Bergen County Judge Honorable Liliana S. DeAvila-Silebi, P.J., Cr and Bergen County Judge Edward A. Jerejian, J.S.C. was not authorized to issue the warrant to retrieve Cell Tower records and search a motor vehicle (**Vin#2C4RC1BG3DR74200**) and install a tracking device, bugging system within the States of New York, Georgia, Virginia, Pennsylvania and North Carolina in this case. The evidence seized pursuant thereto, therefore, must be **Suppressed.**

The warrants were, in the language of the statute, "insufficient on its face" because it was signed by Bergen County Judge Honorable Liliana S. DeAvila-Silebi, P.J., Cr, Bergen County Judge Edward A. Jerejian, J.S.C. in the County of Bergen, New Jersey, authorizing members of Bergen County Prosecutor's office to retrieve Cell Tower records from Cell towers placed in New York, Georgia, North Carolina, Virgina and Pennsylvania; and place an electronic bug and tracking device inside a mini van parked at Budget Rental car, 90-20 Grand Central Parkway, East Elmhurst, NY, NY, 11369--outside of Bergen County Court's jurisdiction.

The jurisdictional language of Title III, it permits a judge to "authoriz[e] or approv[e] interception of wire, oral, or electronic communications within the territorial jurisdiction of the court in which the judge is sitting (and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction)." **18 U.S.C. § 2518(3)**.

It seems reasonable to read the words "**such jurisdiction**" in the phrase as referring back to the jurisdiction in which the judge is sitting; i.e., in this case, the County of Bergen, N.J., since the provision mentions no other jurisdiction. It is also possible that the phrase, by implication, refers to the jurisdiction in which the mobile interception device is installed.

Under either reading, the parenthetical makes clear that a judge cannot authorize the interception of communications if the mobile interception device was not validly authorized, and a device cannot be validly authorized if, at the time the warrant is issued, the property on which the device is to be installed is not located in the authorizing judge's jurisdiction.

According to a Senate Judiciary Committee report, the objective of the language was to ensure that warrants remain effective in the event a target vehicle is moved out of the issuing judge's jurisdiction after a warrant is issued, but before a surveillance device can be placed in the vehicle. **S.Rep. No. 99-541, at 106(a) (1986).**

To the extent that there is uncertainty over the proper interpretation of the statute, **Rule 41** of the Federal Rules of Criminal Procedure, which partially implements the statute, is crystal clear. It states that "a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed." **Fed.R.Crim.P. 41(b)(2).** So, therefore, we have a warrant issued in our case which appears, on its face, to be in violation of the rule (and the statute).

The Supreme Court has repeatedly made clear that the "core concerns" test is a construction of the term "unlawfully intercepted" in paragraph **(i),** not paragraph **(ii)**. Even if we thought that an inquiry into the core concerns of the statute were permitted under paragraph **(ii),** we would, nevertheless, agree with the Fifth Circuit, which recently held that territorial jurisdiction is a core concern of Title III. **United States v. North, 728 F.3d 429, 437 (5th Cir.2013).**

The "jurisdictional flaw in this warrant [cannot] be excused as a technical defect."**United States v. Glover, 736 F.3d 509, 515 (D.C.Cir.2013); see also United States v. Baker, 894 F.2d 1144, 1147 (10th Cir.1990)** (finding a warrant issued by a state court judge to be void because it was outside of his statutory jurisdiction). Even if we assume that an imperfect authorizing order could be thought facially sufficient, we do not see how a blatant disregard of a district judge's jurisdictional limitation can be regarded as only "technical."

Congress has spoken on this issue in the past: The statute requires suppression of evidence gathered pursuant to a facially insufficient warrant. **See United States v. Rice, 478 F.3d 704, 711 (6th Cir.2007).** In any event, it is quite a stretch to label the government's actions in seeking a warrant so clearly in violation of **Rule 41** as motivated by **"good faith." Glover, 736 F.3d at 516** (the magistrate issued a search warrant for a vehicle located outside of his district).

**CONCLUSION**

Therefore, the Defendant Humbly request that this Court does not find the "good faith" exception applicable and instead finds that exclusion of the evidence will serve the "remedial objectives" of the exclusionary rule. **United States v. Leon, 468 U.S. 897, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984).**

## POINT XXIII
## DEFENDANT REQUEST FOR RETURN OF SEIZED PROPERTY OR, ALTERNATIVELY FOR A HEARING

Defendant was indicted on June 17, 2014. The last count of the indictment, seeks forfeiture of property, but fails to give any type of description of the alleged property or Jewelry. On October 10, 2013 and December 23, 2013 the Government obtained a seizure warrant issued by Magistrate Judge Madeline Cox Arleo, Honorable Gerrilyn G. Brill and Honorable Cathy L. Waldor for the seizure of property and jewlery. The Government seized Items from the Defendant's homes, and Hotel room (refer to Exhibit A,B and C) the only problem is the Indictment fails to describe any of the alleged items seized as the alleged stolen property/or Jewelry allegedly involved in this matter.

The issuance of a seizure warrant after the filing of the indictment is a violation of **21 U.S.C.A. Sec. 853(e)(1)** because, under **21 U.S.C.A. Sec. 853(e)(1)**, after an indictment is filed, the Government must seek a restraining order or injunction to preserve property subject to forfeiture. In any event, however, defendant is entitled to a hearing regarding whether the property is subject to seizure at this time under the provisions of **21 U.S.C.A. Sec. 853(e)(2).**

The Defendant's right to a hearing is mandated by his due process rights under the Fifth Amendment.

In **U.S. v. James Daniel Good Real Property, 510 U.S. 43, 114 S. Ct. 492, 126 L. Ed. 2d 490 (1993),** the United States Supreme Court held that a seizure warrant issued for the seizure of real property without notice to the owner and an opportunity for a hearing violated the owner's due process rights. "Our precedents establish the general rule that individuals must receive notice and an opportunity to be heard before the government deprives them of property." **510 U.S. 43, 114 S. Ct. 492**.

Date:

**Mr. Tokyo Gatson/Pro-se Defendant**